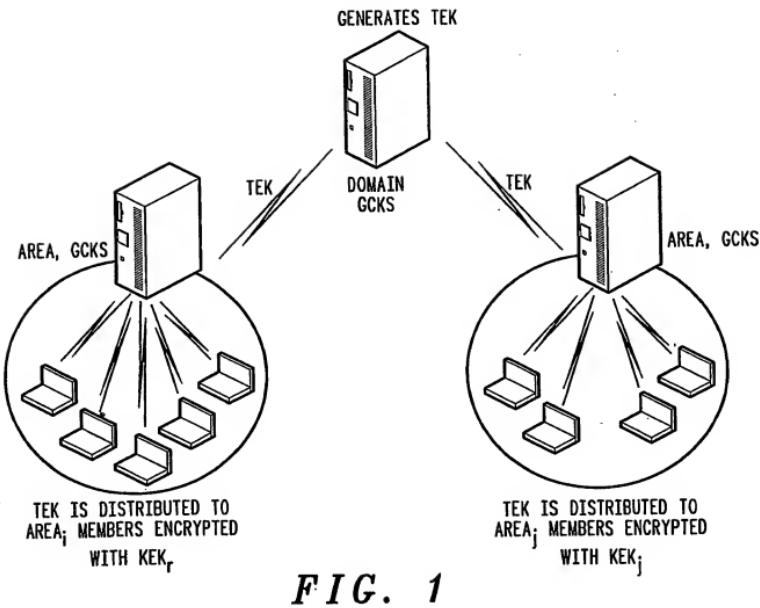


1/7



2/7

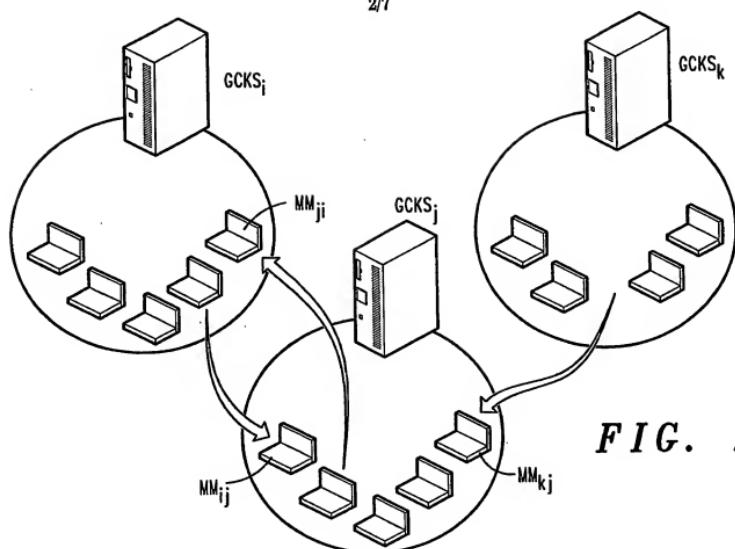


FIG. 2

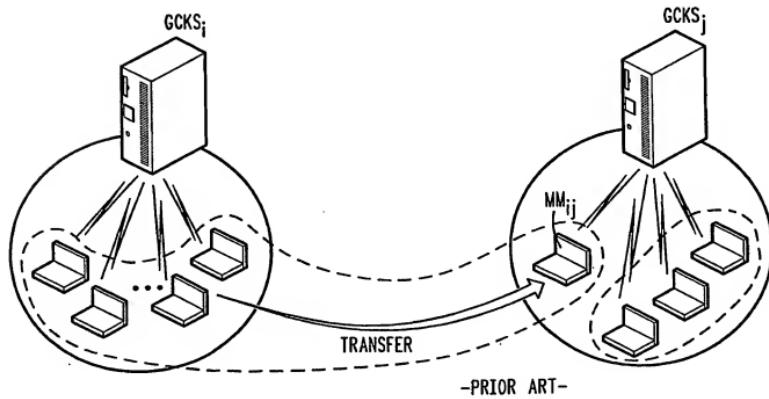
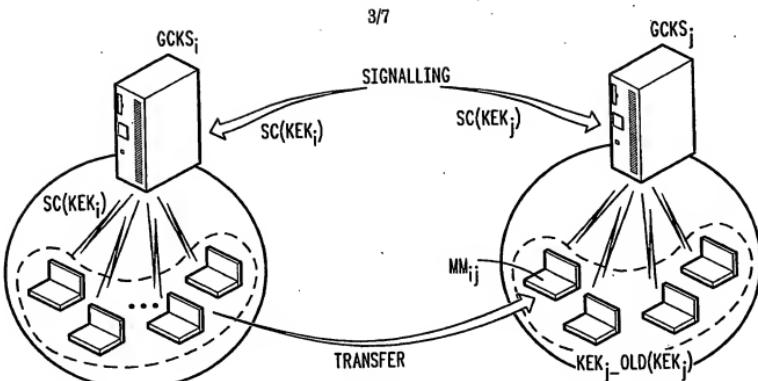
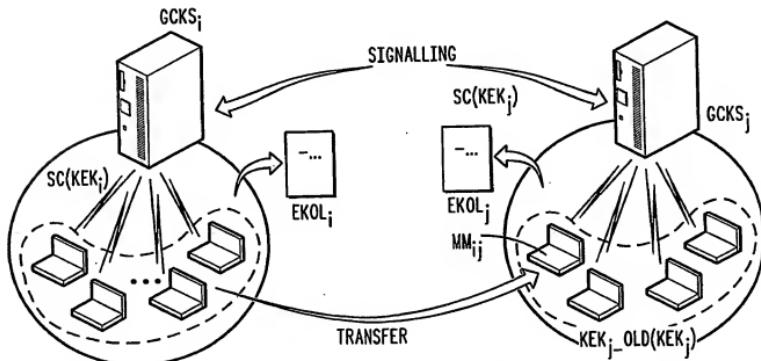


FIG. 3

***FIG. 4******FIG. 5***

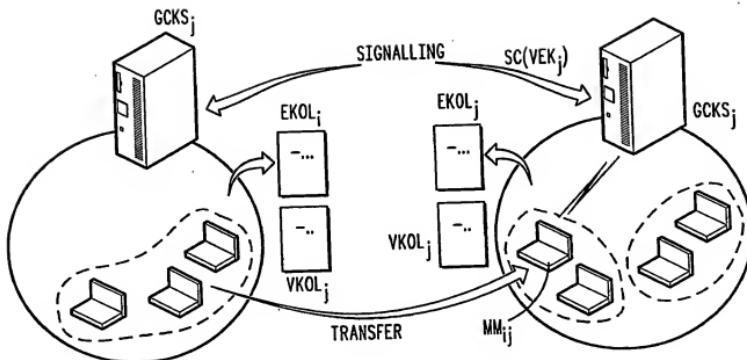


FIG. 6

5/7

FIG. 7

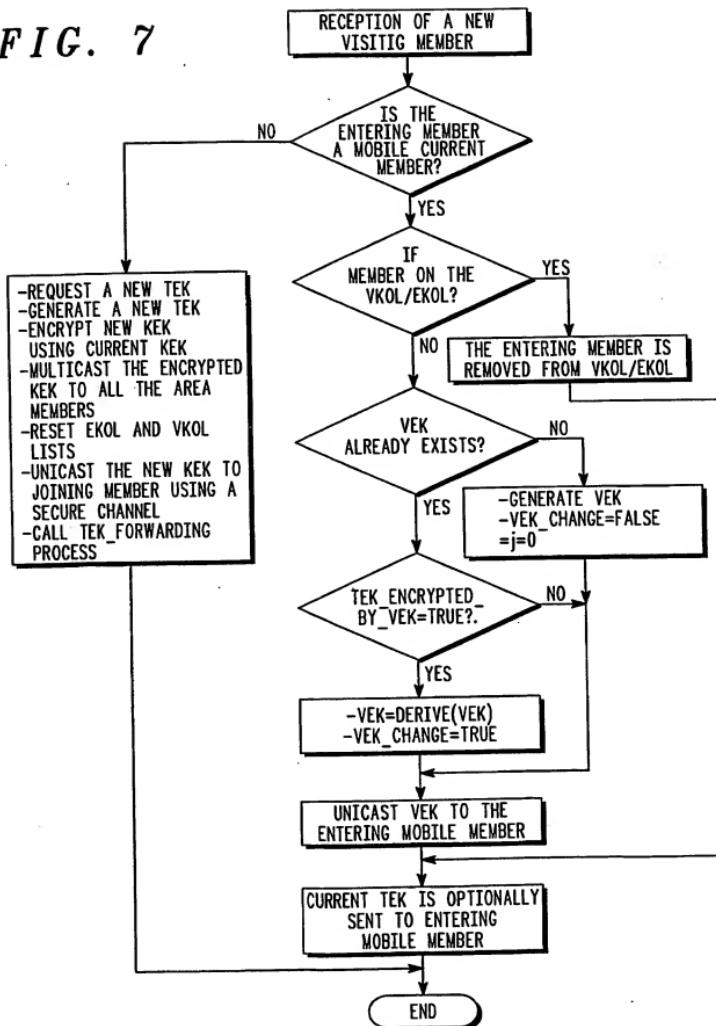


FIG. 8

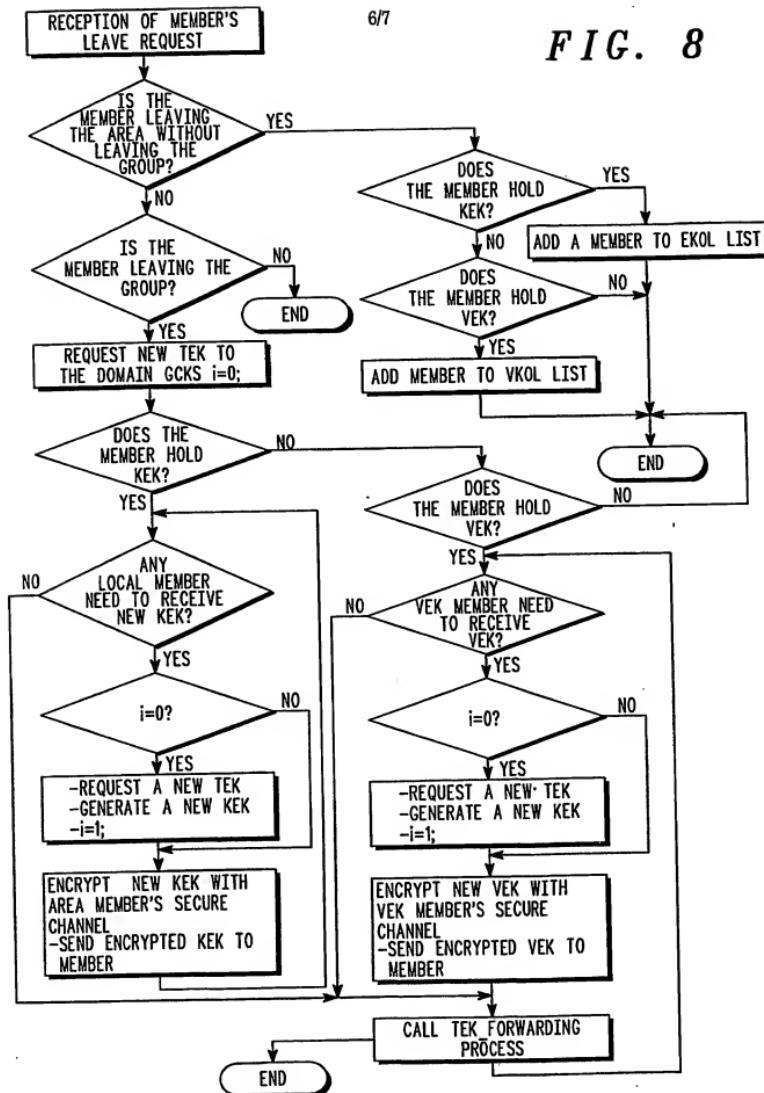


FIG. 9

7/7

RECEPTION OF NEW TEK

ARE
THERE ANY VEK
MEMBERS?

NO

- ENCRYPT TEK WITH KEK
- MULTICAST ENCRYPTED TEK TO AREA MEMBERS

YES

- ENCRYPT TEK WITH KEK
- ENCRYPT TEK WITH VEK
- $j++$; //jINITIALIZEDTO 0
- IF $j=2$; TEK_ENCRYPTED_BY -
VEK=TRUE; $j=0$;
- MULTICAST ENCRYPTED TEK+
"VEK_CHANGE" VALUE TO
AREA MEMBERS

END

RECEPTION OF A NEW TEK

AM I
KEK MEMBER?

YES

DECRYPT THE NEW TEK
USING KEK

NO

VEK_CHANGE=TRUE
AND VEK_USED=TRUE?

NO

VEK=DERIVED(VEK)

YES

- DECRYPT THE NEW TEK
USING VEK
- VEK_USED=TRUE; (CURRENT
VEK WAS USED TO DECRYPT
THE TEK)

END

FIG. 10